



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 6 stycznia 2009 r.

DIS/DEC - 4/174/09

Dot.: [...]

D E C Y Z J A

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r., Nr 98, poz. 1071 z późn. zm.), art. 12 pkt 2, art. 18 ust. 1 pkt 1 i art. 22 w związku z art. 31 ust. 1, art. 36 ust. 2, art. 37, art. 39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz częścią A pkt III ppkt 1 załącznika do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez W.,

nakazuję

W., usunięcie uchybień w procesie przetwarzania danych, poprzez:

- 1. Zawarcie z M. Sp. z o. o., pisemnej umowy powierzenia przetwarzania danych osobowych kandydatów do pracy (przesyłających swoje CV oraz listy motywacyjne), kandydatów na praktyki, bądź osób zgłaszających się z prośbą o pomoc w wyszukaniu pracy, w terminie czternastu dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 2. Opracowanie i wdrożenie polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w terminie czternastu dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**

- 3. Nadaniu upoważnień dla osób dopuszczonych do przetwarzania danych, w terminie siedmiu dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 4. Opracowaniu ewidencji osób upoważnionych do przetwarzania danych osobowych, w terminie siedmiu dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 5. Zabezpieczeniu komputera przenośnego, na którym przetwarzane są dane osobowe kandydatów do pracy (przesyłających swoje CV oraz listy motywacyjne), kandydatów na praktyki, bądź osób zgłaszających się z prośbą o pomoc w wyszukiwaniu pracy przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego w terminie czternastu dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**

U z a s a d n i e

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę we W., zwanej dalej również W. (sygn. akt [...]) w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, tj. ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), zwaną dalej ustawą oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), zwanym dalej rozporządzeniem. W toku kontroli odebrano od pracownika W. ustne wyjaśnienia, skontrolowano systemy informatyczne oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez Prezesa Zarządu W.

Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych, W., jako administrator danych naruszyła przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Przekazaniu M. Sp. z o. o., danych osób poszukujących pracy (przesyłających swoje CV oraz listy motywacyjne), kandydatów na praktyki, bądź osób zgłaszających się z prośbą o pomoc w wyszukiwaniu pracy, bez podstawy prawnej tj. pisemnej umowy powierzenia przetwarzania danych (art. 31 ustawy).
2. Nieopracowaniu polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (art. 36 ust. 2 ustawy).

3. Dopuszczeniu do przetwarzania danych osobowych we W. osób nie posiadających upoważnienia nadanego przez administratora danych (art. 37 ustawy).
4. Nieopracowaniu ewidencji osób upoważnionych do przetwarzania danych osobowych (art. 39 ust. 1 ustawy).
5. Niezabezpieczeniu komputera przenośnego, na którym przetwarzane są dane osobowe kandydatów do pracy oraz kandydatów na praktyki przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

W związku z powyższym, Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy. Pismem z dnia [...] listopada 2008 r. zawiadamiającym o wszczęciu postępowania administracyjnego w przedmiotowej sprawie (nr [...]), administrator danych został poinformowany o prawie czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji wypowiedzenia się co do zebranych dowodów i materiałów oraz zgłoszonych żądań. Pomimo to, W. nie złożyła wyjaśnień oraz nie przedstawiła dowodów potwierdzających usunięcie wskazanych uchybień.

Po zapoznaniu się z całością materiału dowodowego zebranego w sprawie, Generalny Inspektor Ochrony Danych Osobowych zważył co następuje:

Zgodnie z art. 31 ust. 1 ustawy, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.

W toku kontroli ustalono, że obsługą systemu informatycznego (witryny internetowej o adresie [...]) „grzecznościowo” zajmuje się Pan K. Sz., który współpracuje z M. Sp. z o.o. Utrzymaniem (w szczególności aktualizacją, zabezpieczeniem, konfiguracją, modyfikacją treści) ww. witryny zajmuje się Pan K. S. wraz z 2 osobami współpracującymi. Ponadto, serwer pocztowy, na który przesyłana jest poczta, zawierająca CV oraz listy motywacyjne osób poszukujących pracy (znających język [...]), kandydatów na praktyki, bądź osób zgłaszających się z prośbą o pomoc w wyszukaniu pracy, znajduje się w M. Sp. z o.o.

Na podstawie powyższych ustaleń należy stwierdzić, że W. przy przetwarzaniu danych osób poszukujących pracy, (przesyłających swoje CV oraz listy motywacyjne) kandydatów na praktyki, bądź osób zgłaszających się z prośbą o pomoc w wyszukaniu pracy, korzysta z urządzeń (system informatyczny i serwery) znajdujących się w innym podmiocie (M. Sp. o.o.) oraz dopuszcza do sytuacji, w której przetwarzaniem ww. danych zajmują się osoby współpracujące z tym podmiotem. Z tych względów należy uznać, że W. jako administrator danych osobowych przekazuje

przedmiotowe dane M. Sp. z o. o. bez podstawy prawnej, bowiem nie zawarła z ww. podmiotem pisemnej umowy powierzenia przetwarzania danych, o której mowa w art. 31 ustawy.

W myśl art. 36 ust. 2 ustawy, administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1. W myśl § 3 ust. 1 rozporządzenia, na dokumentację, o której mowa w § 1 pkt 1, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Zgodnie z ust. 2, dokumentację, o której mowa w § 1 pkt 1, prowadzi się w formie pisemnej. Natomiast, zgodnie z ust. 3, dokumentację, o której mowa w § 1 pkt 1, wdraża administrator danych.

W toku kontroli ustalono, że kontrolowana jednostka nie opracowała polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Zgodnie z art. 37 ustawy, do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

W toku kontroli ustalono, iż w kontrolowanej jednostce do przetwarzania danych dopuszczone zostały osoby nie posiadające upoważnienia nadanego przez administratora danych.

W myśl art. 39 ust. 1 ustawy, administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:

- 1) imię i nazwisko osoby upoważnionej,
- 2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
- 3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

W toku kontroli ustalono, iż kontrolowana jednostka nie prowadzi ewidencji osób upoważnionych do przetwarzania danych osobowych.

Zgodnie zaś z częścią A, pkt III ppkt 1 załącznika do rozporządzenia, system informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

W toku czynności kontrolnych ustalono, że komputer przenośny, na którym przetwarzane są dane osobowe kandydatów do pracy oraz kandydatów na praktyki nie posiada zainstalowanej ochrony antywirusowej.

Wobec powyższego, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął jak w sentencji.

Decyzja jest ostateczna. Na podstawie art. 21 ust. 1 ustawy o ochronie danych osobowych oraz art. 129 § 2 Kodeksu postępowania administracyjnego, strona niezadowolona z niniejszej decyzji może zwrócić się do Generalnego Inspektora Ochrony Danych Osobowych (adres: ul. Stawki 2, 00-193 Warszawa) z wnioskiem o ponowne rozpatrzenie sprawy, w terminie 14 dni od dnia doręczenia niniejszej decyzji.